Errata/Typos for “Introduction to Modern Cryptography, third edition”

(Last updated April 7, 2022)

Note: negative line numbers correspond to counting from the bottom of the page.

- page 252, line -2 of Construction 7.6: $z_i^*$ should be $y_i^*$.
- page 283, line 11: $\hat{G}(s)$ should be $G(s)$.
- page 362, Exercise 9.24: For this problem, assume that the twisted Edwards representation uses quadratic residue $a$ and quadratic non-residue $d$.
- page 368, line 8: “less than $p_k$” should be “at most $p_k$.”
- page 450, line -4 of Construction 12.36: should read $s \in \{0, 1\}^k$ and $t \in \{0, 1\}^\ell + k$.
- page 483, line -7: $g^{\alpha(s_1^{-1} - s_2^{-1})} = y_1^{r_1 s_1^{-1} - r_2 s_2^{-1}}$ should be $g^{\alpha(s_1^{-1} - s_2^{-1})} = y_2^{r_2 s_2^{-1} - r_1 s_1^{-1}}$.
- page 501, line -12: should read “...we can let $C$ be the set of all strings whose first $m - \log \ell$ bits are all 0 and take $D$ to be the set of all strings whose first $m - 2\log \ell$ bits are all 1.”
- page 577, line -7 should have “$\geq$” instead of “$\leq$.” In any case, the only result we rely on is that when the $\{E_i\}_{i=1}^n$ are disjoint events with $\Pr[\lor_{i=1}^n E_i] = 1$, then for any event $F$ we have
  $$\Pr[F] = \sum_{i=1}^n \Pr[F \land E_i] = \sum_{i=1}^n \Pr[F \mid E_i] \cdot \Pr[E_i].$$
- page 578, line 17: $X_i$ should be $X_1$ and $X_j$ should be $X_2$.
- page 594: Algorithm B.13 is missing “if $b > 0$” on the second-to-last line of the algorithm. In line 13 on the page, the number of modular squarings should be $\|b\| - 1$, not $\|b\|$.

Thanks to Claude Crépeau, Bruno Grenet, Dominique Schröder, and Marek Sefranek for informing us about some of the above typos.